

"Express Mail" mailing label number EV 164034367 US

Date of Deposit: March 16, 2004

Attorney Docket No.15469US01

INTEGRATION OF SECURE IDENTIFICATION LOGIC INTO CELL PHONE

RELATED APPLICATIONS

[0001] [Not Applicable]

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] [Not Applicable]

[MICROFICHE/COPYRIGHT REFERENCE]

[0003] [Not Applicable]

BACKGROUND OF THE INVENTION

[0004] Passwords are a commonly practiced security measure that prevents unauthorized users from accessing computer systems as well as identifying authorized users during an access. However, unauthorized users have used a variety of measures to ascertain the passwords of authorized users.

[0005] Once an unauthorized user has obtained an authorized user's password, the unauthorized user can access the computer system in the same manner as the authorized user. Often times, the unauthorized user accesses the computer system for malicious purposes. The activity of the unauthorized user is generally not detected until significant damage or disruptions have occurred.

[0006] Requiring authorized users to change their passwords at regular intervals can curtail, at least to some extent, the activities of unauthorized users. However, the regular interval time period is usually several weeks or months. During this time period, an unauthorized user can cause significant damage and disruption. Even if the user changes password daily, it could still not be effective to inhibit unauthorized user to do significant damage and disruption for that duration.

[0007] As a result, some computer systems use a time varying randomly generated password for each authorized user. The administrator of the computer system provides each authorized user with a device. The device includes a pseudo-random number generator that generates a code at relatively short time intervals, such as every minute. The computer system is also equipped to determine the pseudo-random number at a given time. When the authorized user seeks to access the computer system, the authorized user uses the code generated and displayed by the device as the password.

[0008] The foregoing provides for quickly changing passwords that are valid for short times. Accordingly, even if an unauthorized user does obtain a password, the password is valid for a very short time period. This significantly curtails the damage that an unauthorized user can do.

[0009] One of the well known disadvantages is associated with providing such device to an authorized user. Given the global reach of the internet, in many cases the device has to be delivered to the user via courier or mail. This can delay initial access by authorized users by

several days. Additionally, when sending the device by mail, it is possible for an unauthorized user to intercept the device.

[0010] Further limitations and disadvantages of convention and traditional approaches will become apparent to one of ordinary skill in the art through comparison of such systems with the present invention as set forth in the remainder of the present application with reference to the drawings.

BRIEF SUMMARY OF THE INVENTION

[0011] Presented herein are systems and methods for integrating secure identification logic into mobile communication devices.

[0012] In one embodiment, there is presented a method for providing a password. The method comprises receiving a registration, wherein said registration includes a phone number associated with a mobile terminal; and transmitting information to the mobile terminal, the password being a function of the information.

[0013] In another embodiment, there is presented a mobile terminal comprising a transceiver, a pseudo-random number generator, a controller, and an output. The transceiver receives a seed from the remote communication device. The pseudo-random number generator generates pseudo-random numbers at regular time intervals based on the seed. The controller provides the seed to the pseudo-random number generator. The output provides passwords based on the pseudo-random numbers at regular time intervals.

[0014] In another embodiment, there is presented a communication system comprising a first node and a second node. The first node receives a seed. The second node transmits the seed, that is into a pseudo-random number generator at a predetermined mobile terminal over a paging channel.

[0015] These and other advantages and novel features of the present invention, as well as details of an illustrated embodiment thereof, will be more fully understood from the following description and drawings.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

[0016] **FIGURE 1** is a block diagram of a communication system for configuring a mobile terminal to provide a time varying random password in accordance with an embodiment of the present invention;

[0017] **FIGURE 2** is a block diagram of an exemplary Global System for Mobile Communication Public Land Mobile Network that can be used in accordance with an embodiment of the present invention;

[0018] **FIGURE 3** is a block diagram of an exemplary mobile terminal in accordance with an embodiment of the present invention;

[0019] **FIGURE 4** is a signal flow diagram for configuring a mobile terminal to provide a time varying random password in accordance with an embodiment of the present invention; and

[0020] **FIGURE 5** is a signal flow diagram for configuring a mobile terminal to provide a time varying random password in accordance with another embodiment of the present invention

DETAILED DESCRIPTION OF THE INVENTION

[0021] Referring now to **FIGURE 1**, there is illustrated a block diagram of an exemplary communication system for configuring a mobile terminal to provide a time varying random password in accordance with an embodiment of the present invention. The system includes a computer network 100 and a wireless phone network 150.

[0022] The communication system includes a server 105 that is accessible over a network 100 by a client terminal 115. The network 110 can comprise any combination of a variety of communication media, such as, but not limited to, the internet, the public switched telephone network, a local area network (LAN), and a wide area network (WAN).

[0023] The server 105 may provide access to a database storing sensitive information or the like, or allow individuals to perform various transactions. Accordingly, it is important to control access to the server 105. As a result, the server 105 requires a password from the client terminal 115 that validates the identity of the user at the client terminal 115.

[0024] However, unauthorized users have been known to use a variety of measures to obtain the password of an authorized user. With the password, the unauthorized user often proceeds to access the server 105 for malicious purposes.

[0025] To curtail this, the server 105 uses a time-varying pseudo-random password. A pseudo-random number generation algorithm generates the time-varying pseudo-random password at relatively short intervals, such as every minute or even less depending on the granularity

required for the desired password security. Accordingly, even if an unauthorized user succeeds in obtaining an authorized user's password, the password is only valid for the remainder of the short interval.

[0026] The pseudo-random number generation algorithm can be implemented at the server 105 in one of a number of ways. For example, an Application Specific Integrated Circuit (ASIC) can also be incorporated into the server 105 that continuously runs the pseudo-random number generation algorithm. Alternatively, the pseudo-random number generation algorithm can be incorporated as software at the server 105.

[0027] The authorized user receives the time varying pseudo-random password from a mobile terminal 120. The logic that implements the pseudo-random number generation algorithm is integrated into the mobile terminal 120. This logic could either be an ASIC or a part of an ASIC present in the mobile terminal 120 or part of a software program running at the mobile terminal 120. The mobile terminal 120 displays the current time-varying pseudo-random password on its display screen. Therefore, when an authorized user seeks access to the server 105, via client 115, the authorized user provides the time-varying pseudo-random password displayed by the mobile terminal 120. The server 105 then compares the time-varying pseudo-random password provided by the authorized user to the pseudo-random number generated by the pseudo-random number generation algorithm at the server 105. The server 105 allows access, if there is an exact match.

[0028] In order for the pseudo-random number generation algorithm at the server 105 to provide the same pseudo-

random numbers as the mobile terminal 120 at the same times, the pseudo-random number generation algorithms are the same and synchronized.

[0029] The pseudo-random number generation algorithm requires an input called 'seed' to generate the pseudo-random numbers. The seed can be provided by an external source to the pseudo-random number generation algorithm. The pseudo-random number generation algorithm generates the first pseudo-random number from that seed, then generates the second pseudo-random number from the first pseudo-random number thereafter, etc.

[0030] As can be seen, the sequence of pseudo-random numbers generated by the pseudo-random number generation algorithm is dependent on the seed. Additionally, different seeds to the same pseudo-random number generation algorithms result in different sequences of pseudo-random numbers. In fact, the same pseudo-random number generation algorithm can provide different time-varying pseudo-random passwords to any number of users, by assigning each user with a different seed. In order to ensure uniqueness of the sequence of pseudo-random numbers to each user, the size of the pseudo-random number generated also plays a significant role.

[0031] When a user at the client terminal 115 initially registers to access the server 105, the registration can include either a phone number or any other identification number associated with the user's mobile terminal 120. The server 105 can select a seed for the user. As an added security measure, the server 105 can select the seed based on the time of registration. The server 105 can then use a terminal 125 with access to a cellular phone network 130.

The terminal 125 transmits the seed to the mobile terminal 120 using the cellular phone network 130. The terminal 125 can access the cellular phone network 130, either directly, or via a public switched telephone network.

[0032] For example, in one embodiment, the terminal 125 establishes a phone call to the mobile terminal 120. When the phone call is established, the terminal 125 can transmit audible signals over the cellular phone network 130 representing the seed. The mobile terminal 120 can accordingly, load the seed into the pseudo-random number generator at a predetermined time in synchronization with the server 105. The predetermined time is preferably proximate to the time of transmission, such as at the next minute interval, taking into consideration the path delay time of communication from server 105 to mobile terminal 120.

[0033] In another embodiment, the terminal 125 can cause the cellular phone network 130 to transmit control signals indicating the seed to the mobile terminal 120. The mobile terminal 120 can accordingly load the seed into the pseudo-random number generator at a predetermined time in synchronization with the server 105.

[0034] The cellular phone network 130 can comprise a variety of wireless telecommunications networks, such as, but not limited to, the Global System for Mobile (GSM) Communications, or the Personal Communication Services (PCS) network, Code Division Multiple Access (CDMA) network, IEEE 802.11 Wireless LAN network, Bluetooth network etc.

[0035] Referring now to FIGURE 2 there is illustrated a block diagram of a Global System for Mobile Communication (GSM) Public Land Mobile Network (PLMN) 210. The PLMN 210 is composed of a plurality of areas 212, each with a node known as a Mobile Switching Center (MSC) 214 and an integrated Visitor Location Register (VLR) 216 therein. The MSC/VLR areas 212, in turn, include a plurality of Location Areas (LA) 218, which are defined as that part of a given MSC/VLR area 212 in which a mobile terminal 120 may move freely without having to send update location information to the MSC/VLR area 212 that controls the LA 218. Each Location Area 212 is divided into a number of cells 222. The mobile terminal 120 is the physical equipment, e.g., a car phone or other portable phone, used by mobile subscribers to communicate with the cellular network 210, each other, and users outside the subscribed network, both wireline and wireless.

[0036] The MSC 214 is in communication with at least one Base Station Controller (BSC) 223, which, in turn, is in contact with at least one Base Transceiver Station (BTS) 224. The BTS is a node comprising the physical equipment, illustrated for simplicity as a radio tower, that provides radio coverage to the geographical part of the cell 222 for which it is responsible. It should be understood that the BSC 223 may be connected to several base transceiver stations 224, and may be implemented as a stand-alone node or integrated with the MSC 214. In either event, the BSC 223 and BTS 224 components, as a whole, are generally referred to as a Base Station System (BSS) 225. At least one of the MSCs 214 are connected to the public switched telephone network (PSTN).

[0037] The PLMN Service Area or wireless network 210 includes a Home Location Register (HLR) 226, which is a database maintaining all subscriber information, e.g., user profiles, current location information, International Mobile Subscriber Identity (IMSI) numbers, and other administrative information. The HLR 226 may be co-located with a given MSC 214, integrated with the MSC 214, or alternatively can service multiple MSCs 214, the latter of which is illustrated in **FIGURE 2**.

[0038] The VLR 216 is a database containing information about all of the mobile terminals 120 currently located within the MSC/VLR area 212. If a mobile terminal 120 roams into a new MSC/VLR area 212, the VLR 216 connected to that MSC 214 will request data about that mobile terminal 120 from the HLR database 226 (simultaneously informing the HLR 226 about the current location of the mobile terminal 120). Accordingly, if the user of the mobile terminal 120 then wants to make a call, the local VLR 216 will have the requisite identification information without having to re-interrogate the HLR 226. In the afore-described manner, the VLR and HLR databases 216 and 226, respectively, contain various subscriber information associated with a given mobile terminal 120.

[0039] In one embodiment, the terminal 125 can establish a phone call with the mobile terminal 120 over the GSM PLMN 210, either directly or via the PSTN. Upon establishing the phone call, the terminal 125 transmits audio signals to the mobile terminal 120 causing the mobile terminal 120 to load a particular seed to the pseudo-random number generator. Alternatively, the terminal 125 can cause one of the MSCs 214 to transmit a control signal, via a base station 224

to the mobile terminal 120, causing the mobile terminal 120 to load a particular seed to the pseudo-random number generator. These are few of the many possible techniques of loading the seed to the psuedo-random number generation logic in the mobile terminal 120.

[0040] Transmitting the seed during an established call can be facilitated by the establishment of a predetermined communication protocol for secured communication between the terminal 125 and the mobile terminal 120. Such predetermined protocol can include transmission of an arbitrary control signal indicating to the mobile terminal 120 that the seed will be transmitted subsequently. Upon receipt of the foregoing arbitrary control signal, the mobile terminal 120 prepares to receive the seed and loads the seed into the pseudo-random number generator. The communication between terminal 125 and mobile terminal 120 can be made secured by employing secured communication protocols such as but not limited to, the protocols using digital certificates like Transport Layer Security (TLS) protocol, Secure Socket Layer (SSL) protocol etc.

[0041] Transmitting a control signal from a particular one of the MSCs 214 to the mobile terminal 120 may be facilitated by adapting the preexisting protocol to define commands that cause the mobile terminal 120 to load a particular seed to a pseudo-random number generator incorporated therein. For example, the MSC 214 can transmit a command to load a seed at a particular predetermined time, along with the seed, to the mobile terminal 120 over a paging channel. For added security, a secure paging channel can be used. Upon receiving the foregoing signal, the mobile terminal 120 loads the seed into the pseudo-

random number generator at the predetermined time. After receiving the seed, the mobile terminal 120 can transmit an acknowledgement to the MSC 214 using a random access channel.

[0042] Referring now to **FIGURE 3**, there is illustrated a block diagram describing an exemplary mobile terminal 120 in accordance with an embodiment of the present invention. For purposes of clarity, the block diagram is not intended as an exhaustive illustration, and certain components may be omitted.

[0043] The mobile terminal 120 comprises a controller 305, non-volatile memory 307, a keypad 310, a transceiver 315, a speaker 317, a microphone 318, an output such as a visual screen 320 or interface port 321, and a pseudo-random number generator 325. The pseudo-random number generator 325 generates a pseudo-random number at regular intervals that are controlled by a system clock 330. The controller 305 causes the current time varying pseudo-random password to be displayed on the screen 320.

[0044] The time varying pseudo-random password can be the pseudo-random number generated by the pseudo-random number generator 325. Alternatively, the time varying pseudo-random password 305 can be derived from the pseudo-random number generated from the pseudo-random number generator 325. For example, in cases where the pseudo-random number is lengthy, the controller 305 may truncate a portion of the pseudo-random number or perform other types of mathematical operations for reducing its length.

[0045] The time-varying pseudo-random password as well as a user identification can be provided in a variety of

ways. In one embodiment, the time varying pseudo-random password can be output to the interface port 321. The interface port 321 can be connected to a computer such as the client terminal 115. Connecting the interface port 321 to the client terminal 115 can cause the time varying pseudo-random password to be displayed on a screen associated with the client terminal 115. In another embodiment, the time-varying pseudo-random password can continuously be displayed on the screen 320. In another embodiment, the user may request the current time-varying pseudo-random password using the keypad 310 with the assistance of a graphical user interface provided on the screen 320.

[0046] The pseudo-random number generator 325 can comprise, for example, a circuit, such as a linear feedback shift register (LFSR), that generates pseudo-random numbers. Alternatively, the pseudo-random number generator can be implemented by a processor executing a set of instructions, wherein execution of the sets of instructions causes implementation of the pseudo-random number generation algorithm.

[0047] Additionally, there can be varying levels of integration between the pseudo-random number generator 325 and the controller 305. For example, the controller 305 and the pseudo-random number generator 325 can be separate integrated circuits that are fused together at board level. Alternatively, the controller 305 and the pseudo-random number generator 325 can be integrated together in an integrated circuit.

[0048] As noted above, the seed for the pseudo-random number generator 325 is provided by the cellular phone

network 130. The mobile terminal 120 receives radio signal from the cellular phone network 130 via the transceiver 315. Various demodulation, signal processing and deciphering can be performed to recover the seed.

[0049] The mobile terminal 120 generally operates in one of two modes - a paging mode and an active mode. Generally, the paging mode is associated with the times that the mobile terminal 120 is not engaged in a phone call, while the active mode is associated with the times that the mobile terminal 120 is engaged in a phone call.

[0050] During the paging mode, the mobile terminal 120 scans a paging channel at regular time intervals for any communications from the cellular phone network 130. The communications can include for example, a request for a phone connection, a time indicator, quality of service signaling, and roaming notifications, just to name a few.

[0051] The paging channel is made secured by employing security protocols based on Public Key Cryptography technique. The example of such protocols are TLS, SSL etc. These protocols exchange digital certificates for authentication, and at the end of the authentication process a unique session key is derived which is used to encrypt the seed at the transmitter end and decrypt the seed at the mobile terminal 120.

[0052] In one embodiment of the present invention, a command is defined and an MSC 214 transmits the command, a seed, and a time over the paging channel to the mobile terminal 120. Receipt of the command by the mobile terminal 120 causes the mobile terminal 120 to load the seed into the pseudo-random number generator 325 at the provided

time. Additionally, the mobile terminal 120 transmits an acknowledgment via the transceiver 315.

[0053] Accordingly, the non-volatile memory 307 can include instructions for detecting and performing the foregoing actions responsive to receiving the command. The foregoing instructions can be incorporated as part of a paging mode program.

[0054] In another mode, receipt of the command by the mobile terminal 120 can cause an interrupt in the paging mode program. The interrupt handler for the interrupt can cause the seed to be loaded into the pseudo-random number generator 325 at the provided time.

[0055] In another embodiment, the mobile terminal 120 can receive the seed during establishment of a phone call from the cellular phone network 130. As noted above, a predetermined communication protocol for communication between the terminal 125 and the mobile terminal 120 can include transmission of an arbitrary control signal indicating to the mobile terminal 120 that the seed will be transmitted subsequently. The non-volatile memory 307 can include instructions for detecting the arbitrary control signal and acting on the arbitrary control signal. Upon detecting the arbitrary control signal, the mobile terminal 120 prepares to receive the seed and a time. Upon receiving the seed and the time, the mobile terminal 120 loads the seed into the pseudo-random number generator 325 at the given time.

[0056] Referring now to **FIGURE 4**, there is illustrated a signal flow diagram for providing a seed and time to a pseudo-random number generator in accordance with one

embodiment of the present invention. During the initial registration (signal 405), the user provides the phone number associated with their mobile terminal. Responsive thereto, the server 105 allocates a seed for the user and determines a synchronization time.

[0057] The server 105, via the terminal 125 transmits the phone number, a seed, and a synchronization time (signal 410) over the cellular phone network 130. The infrastructure of the cellular phone network 130 identifies and locates the mobile terminal 120 associated with the phone number, and routes the phone number, seed and synchronization time to an MSC 214 in proximity to the mobile terminal 214. The MSC 214 causes a base station to transmit the seed and the synchronization time and a command to load the seed at the synchronization time (signal 415) to the mobile terminal 120 using a paging channel.

[0058] Upon receipt of the seed and the synchronization time, the mobile terminal 120 sends an acknowledgement (signal 420) to the MSC 214 using a random access channel, that is relayed back to the server 105. The mobile terminal 120 waits for the synchronization time (425). At the synchronization time, the mobile terminal 120 and the server 105 load the seed into their respective pseudo-random number generators (430).

[0059] After the seed is loaded into the pseudo-random number generator, the mobile terminal 120 screen can display a time varying pseudo-random password. An authorized user at client terminal 115 establishes a client server connection by providing the time varying pseudo-random password (signal 435) displayed on the mobile

terminal 120 screen. The server 105 compares (440) the password received from the client terminal 115 to a pseudo-random number generator at the server 105. If the foregoing match, the server grants access (signal 445) to the client terminal 115.

[0060] Referring now to **FIGURE 5**, there is illustrated a signal flow diagram for providing a seed and time to a pseudo-random number generator in accordance with one embodiment of the present invention. During the initial registration (signal 505), the user provides the phone number associated with their mobile terminal. Responsive thereto, the server 105 allocates a seed for the user and determines a synchronization time.

[0061] The server 105 via terminal 125 requests an outgoing phone call (signal 510) to the phone number provided during the registration. The infrastructure of the cellular phone network 130 identifies and locates the mobile terminal 120 associated with the phone number. An MSC 214 in proximity to the mobile terminal 214 pages (signal 515) the mobile terminal 120 using a paging channel.

[0062] Upon receiving the page, the mobile terminal 120 alerts the user to answer the call. Upon the user's answer, a phone call is established between the server 105/terminal 125 and the mobile terminal 120. The server 105/terminal 125 transmits audio signals indicating a command (signal 525) to load the subsequent seed at the indicated time (signal 530).

[0063] The mobile terminal 120 waits (535) until the provided synchronization time 535 and loads (540) the seed

into the pseudo-random number generator. Likewise the server 105 loads (540) the seed into a pseudo-random number generator, thereat.

[0064] After the seed is loaded into the pseudo-random number generator, the mobile terminal 120 screen can display a time varying pseudo-random password. An authorized user at client terminal 115 establishes a client server connection by providing the time varying pseudo-random password (signal 545) displayed on the mobile terminal 120 screen. The server 105 compares (550) the password received from the client terminal 115 to a pseudo-random number generator at the server 105. If the foregoing match, the server grants access (signal 555) to the client terminal 115.

[0065] While the present invention has been described with reference to certain embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the scope of the present invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the present invention without departing from its scope. Therefore, it is intended that the present invention not be limited to the particular embodiment disclosed, but that the present invention will include all embodiments falling within the scope of the appended claims.